REMARKS

In view of the following discussion, none of the claims now pending in the application are unpatentable under the provisions of non-statutory obviousness type double patenting and 35 U.S.C. §§ 101 and 103. Claims 1, 8 and 15 are amended. Support for the amendment may be found in the specification on at least page 5, lines 20-22. In addition, various amendments were made to address informalities. No new matter was added. Thus, all of the claims are now in allowable form.

I. REJECTION OF CLAIMS 1, 8 AND 15 UNDER 35 U.S.C. § 101

The Examiner rejected claims 1, 8 and 15 under 35 U.S.C. § 101 as being the same as claim 1 of U.S. Patent No. 7,444,417 (hereinafter the '417 patent). The rejection is traversed.

The Examiner's attention is directed to the fact that claim 1 of the '417 patent and the claims 1, 8 and 15 of the present application are not the same. For example, claim 1 of the '417 patent does not refer to any virtual private networks nor does it recite the limitation of "a virtual private network application in communication with a first one of the plurality of edge routers, the virtual private network application having a first internet protocol address" or any limitation about injecting border gateway protocol routing instructions. In fact, none of the limitations of claim 1 of the '417 patent and claims 1, 8 and 15 of the present application are the same. Therefore, claims 1, 8 and 15 fully satisfy the requirements for double patenting under 35 U.S.C. § 101 and the rejection should be withdrawn.

II. REJECTION OF CLAIMS 1-3, 8 AND 15 UNDER NON-STATUTORY OBVIOUSNESS-TYPE DOUBLE PATENTING

The Examiner provisionally rejected claims 1-3, 8 and 15 as being unpatentable over claims 1, 3, 12 and 14 of co-pending application no. 12/284,254. Responsive to the Examiner, a terminal disclaimer is filed herewith

including the correct filing date of co-pending application no. 12/284,254 to overcome the rejection. As such, the rejection should be withdrawn.

III. REJECTION OF CLAIMS 1-8 AND 10-19 UNDER 35 U.S.C. § 103

The Examiner rejected claims 1-8 and 10-19 as being unpatentable over Talpade, et al. (U.S. Patent Publication No. 2004/0148520, published on July 29, 2004, hereinafter referred to as "Talpade") in view of Munger, et al. (U.S. Patent No. 6,618,761, issued on September 9, 2003, hereinafter referred to as "Munger") and Iljitsch van Beijnum (O'Reilly Media, Inc., allegedly published on September 11, 2002, hereinafter referred to as "BGP"). It should be noted that the Examiner only listed claims 1, 3, 5-8, 11-15, 17 and 19 in the heading of the rejection but appears to have intended to reject all claims under the present rejection based upon the detailed rejection. Under such assumption the rejection is traversed.

Talpade discloses mitigating denial of service attacks. Talpade discloses rerouting all traffic from all routers to a filter router when a denial of service attack is detected. (See Talpade, Abstract).

Munger discloses an agile network protocol for secure communications with assured system availability. Methods and systems for allowing a plurality of computer nodes to communicate using weighted transmission paths are provided. (See Munger, Abstract).

BGP discloses a general disclosure of BGP protocol. (See BGP, §2.3).

The Examiner's attention is directed to the fact that Talpade, Munger, and BGP, either alone or in any permissible combination, fail to describe or suggest a network or method comprising a router for injecting a routing instruction or a second internet protocol address comprising a routing instruction having a same internet protocol address as a first internet protocol address, but with a higher preference value than the first internet protocol address and having a community value such that a selected first number of edge routers direct virtual private network traffic addressed for the first internet protocol address to the virtual private network application and a selected second number of edge routers direct

virtual private network traffic addressed for the second internet protocol address to the black-hole router, wherein virtual private network traffic received by the black-hole router is black-holed, as positively claimed by the independent claims. Specifically, independent claims 1, 8 and 15 positively recite:

1. An internet service provider virtual private network network comprising:
a plurality of edge routers;
a plurality of core routers for allowing communication between ~~said~~ the plurality of edge routers;
a virtual private network application in communication with a first one of the plurality of edge routers, the virtual private network application having a first internet protocol address; and
a black-hole router in communication with the plurality of core routers, wherein virtual private network traffic received by the black-hole router is black-holed, the black-hole router for injecting a second IP address into the internet service provider virtual private network, the second internet protocol address comprising:
a same internet protocol address as the first internet protocol address;
a higher preference value than the first internet protocol address; and
a community value such that when the second internet protocol address is injected, a selected first number of edge routers direct virtual private network traffic addressed for the first internet protocol address to the virtual private network application and a selected second number of edge routers direct virtual private network traffic addressed for the second internet protocol address to the black-hole router.

8. An internet service provider network comprising:
a plurality of edge routers;
an application in direct or indirect electrical communication with a first one of the plurality of edge routers;
the application having a first internet protocol address such that virtual private network traffic addressed for the first internet protocol address and entering the internet service provider network at any one of the plurality of edge routers, is routed to the application;
a black-hole router, wherein virtual private network traffic received by the black-hole router is black-holed; and
a router for injecting an instruction into the internet service provider network, such that a select edge router redirects virtual private network traffic, which is addressed to the first internet protocol address, to the black-hole router, wherein ~~said~~ the injected instruction comprises a routing

instruction having a same IP internet protocol address as the first internet protocol address, but with a higher preference value than the first internet protocol address and having a community value.

15. A method of managing a distributed denial of service attack on an application within an internet service provider network, the application having a first internet protocol address, the method comprising:

injecting a border gateway protocol routing instruction into the internet service provider network when the distributed denial of service attack is occurring, the border gateway protocol routing instruction comprising a second internet protocol address having a same internet protocol address as the first internet protocol address, but with a higher preference value than the first internet protocol address and having a community value;

redirecting, at a selected edge router, virtual private network traffic addressed for the second internet protocol address to a black-hole router, wherein the virtual private network traffic received by the black-hole router is black-holed; and

directing, at another edge router, virtual private network traffic addressed for the first internet protocol address to the application that is experiencing the distributed denial of service attack.

In one embodiment of the disclosure, a network or method comprising a router for injecting a routing instruction or a second internet protocol address comprising a routing instruction having a same internet protocol address as a first internet protocol address, but with a higher preference value than the first internet protocol address and having a community value such that a selected first number of edge routers direct virtual private network traffic addressed for the first internet protocol address to the virtual private network application and a selected second number of edge routers direct virtual private network traffic addressed for the second internet protocol address to the black-hole router, wherein virtual private network traffic received by the black-hole router is black-holed is provided. For example, traffic is selectively re-routed to one or more edge routers by using preference and community values of an injected instruction or second IP address that is identical to a first address. (See e.g., specification, p. 11, l. 16 – p. 12, l. 5).

The alleged combination (as taught by Talpade) fails to render obvious the independent claims because the alleged combination fails to describe or suggest

a network or method comprising a router for injecting a routing instruction or a second internet protocol address comprising a routing instruction having a same internet protocol address as a first internet protocol address, but with a higher preference value than the first internet protocol address and having a community value such that a selected first number of edge routers direct virtual private network traffic addressed for the first internet protocol address to the virtual private network application and a selected second number of edge routers direct virtual private network traffic addressed for the second internet protocol address to the black-hole router, wherein virtual private network traffic received by the black-hole router is black-holed. Claims 1, 8 and 15 were amended to further define the black hole router. Notably, the claims now recite that traffic received at the black hole router is "black-holed". In other words, traffic does not escape or is not forwarded out of the black hole router.

In view of this clarifying amendment, it should be noted that Talpade teaches away from the claims. The claims specify that only a select number of edge routers (i.e., less than all or a subset of all the routers) are instructed to re-direct traffic to the black hole router, while the remaining routers continue to forward traffic to the VPN application. Thus, only some of the VPN traffic is diverted to the black hole router.

In stark contrast, Talpade explicitly states that **all traffic** is redirected to the router filter. Talpade discloses "[t]he new routing information instructs the border and edge routers to reroute all DDoS and non-DDoS traffic directed at the customer network under attack to the filter router using the IP-in-IP tunnels. (See Talpade, para. [0009], emphasis added). As noted above, the claims specify that the injected routing instruction contains a second IP address that is the same as the first IP address, but having a higher preference value and a community value. In other words, all traffic is still forwarded to the system under attack. However, once it reaches the system under attack, only some of the traffic is diverted to the black hole router, while the remaining traffic is forwarded to the VPN application. In other words, unlike Talpade, the present disclosure only diverts a portion of the VPN traffic destined for the system under attack to the black hole router.

The Examiner is reminded that the MPEP § 2141.02(VI) requires the Examiner to consider the prior art in its entirety. "A prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention". MPEP § 2141.02(VI), W.L. Gore & Associates, Inc., v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed Cir. 1983), cert. denied, 469 U.S. 851 (1984). Thus, using Talpade with any combination of other references would still teach away from the present claims. The Examiner is expressly prohibited from ignoring those portions of Talpade that explicitly teach away from the present claims.

Moreover, the Examiner concedes that Talpade fails to describe or suggest the above limitation in the Office Action. (See Office Action, p. 3, §4). However, the Examiner asserts that Munger and BGP bridge the substantial gap left by Talpade.

Munger and BGP fail to bridge the substantial gap left by Talpade because Munger and BGP also fail to describe or suggest a network or method comprising a router for injecting a routing instruction or a second internet protocol address comprising a routing instruction having a same internet protocol address as a first internet protocol address, but with a higher preference value than the first internet protocol address and having a community value such that a selected first number of edge routers direct virtual private network traffic addressed for the first internet protocol address to the virtual private network application and a selected second number of edge routers direct virtual private network traffic addressed for the second internet protocol address to the black-hole router, wherein virtual private network traffic received by the black-hole router is black-holed. In view of the amendments, Munger also teaches away from the present claims. The Examiner asserts that the TARP routers disclosed by Munger are equivalent to a black hole router recited by the present claims. Notably, a black hole router is adapted to black hole traffic (i.e. the traffic is trapped and not forwarded at the black hole router). This language was amended into the independent claims to further define the black hole router.

In stark contrast, the TARP routers by Munger are designed to forward packets randomly to make communication private. (See Munger, col. 7, l. 40 – col. 9, l. 19). That is, the TARP routers taught by Munger do not "black hole" traffic. Thus, the TARP routers are not equivalent to a black hole router.

In addition, the TARP routers disclosed by Munger do not inject a second IP address into said ISP VPN network. Rather, Munger discloses that the TARP routers interleave data packets and create new packets that have headers identical to the original data packets. (See Munger, col. 9, ll. 36-50). Notably, the claims do not recite creating new packets having a second IP address.

Furthermore, the method disclosed by Munger would not be practical for the black hole router of the present disclosure. For example, the present disclosure is designed to stop attack traffic. Thus, using the method disclosed by Munger would further slow down the computer network because the router would be required to interleave each one of the thousands of incoming packets during an attack and create new packets for each of the original packets.

In stark contrast, the claims recite that the black hole router simply injects the second IP address into the ISP VPN network. For example, when routers are identified as potentially being the source of the attack traffic, the second IP address may be injected into the network by updating the routing tables of the routers in question. As a result, the packets do not need to be manipulated, but simply routed based upon the routing protocols of the suspected router or routers.

In addition, the Examiner concedes that Talpade and Munger fail to describe or suggest a second IP address comprising a routing instruction having a same internet protocol address as a first internet protocol address, but with a higher preference value than the first internet protocol address and having a community value such that a selected first number of edge routers direct virtual private network traffic addressed for the first internet protocol address to the virtual private network application and a selected second number of edge routers direct virtual private network traffic addressed for the second internet protocol address to the black-hole router, wherein virtual private network traffic received

by the black-hole router is black-holed. However, the Examiner asserts that BGP discloses the above limitations. However, BGP does not describe or suggest using these values to selectively re-direct traffic to a black hole router. Thus, the combination of Talpade, Munger and BGP fails to render obvious independent claims 1, 8 and 15.

In addition, dependent claims 2-7, 10-14 and 16-19 depend from independent claims 1, 8 and 15, respectively, and recite additional limitations. As such, and for the exact same reason set forth above, claims 2-7, 10-14 and 16-19 are also patentable over Talpade, Munger and BGP and respectfully request the rejection be withdrawn.

CONCLUSION

Thus, all of the claims now fully satisfy the requirements of non-statutory obviousness type double patenting and 35 U.S.C. §§ 101 and 103. Consequently, all the claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 542-2280x130 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully Submitted,

October 7, 2010

Wall & Tong, LLP
25 James Way
Eatontown, New Jersey 07724

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 542-2280, Ext. 130